

T-NEX Fraud Detection: Transaktionsüberwachung und Fallbearbeitung

Version des Steckbriefs: 1.0 · 11. September 2026

Dokumentierter Funktionsstand: 30. August 2026 · Anwendungsversion 15.23.0

T-NEX Fraud Detection unterstützt Institute dabei, auffällige Transaktionsmuster zu erkennen, Alarmer je Kunde zu bündeln und die fachliche Entscheidung nachvollziehbar zu dokumentieren. Das Produkt verbindet konfigurierbare Regeln, Belegtransaktionen, KI-gestützte Triage und einen Prüfpfad für die Fallbearbeitung.

Geldwäschemonitoring und Karten- beziehungsweise Zahlungsbetrug werden als getrennte Aufgabenfelder behandelt. Das Modul **erkennt und dokumentiert**. Es blockiert keine Zahlungen und sperrt keine Karten.

Dokumentierter Funktionsumfang

Bereich	Was das Modul unterstützt
Transaktionsaufnahme	Übernahme von Buchungen über eine Schnittstelle, Dublettenerkennung anhand der externen Transaktionskennung
Regelwerk	Neun dokumentierte Typologien mit konfigurierbaren Parametern, etwa Strukturierung, schnelle Durchleitung und auffällige Kartenfrequenz
Alarmer	Dokumentation des Regelauslösers mit Kategorie, Schweregrad und Belegtransaktionen
KI-Triage	Risikowert, Begründung und Handlungsempfehlung sowie Kennzeichnung von Modell und Prompt-Version
Fallsteuerung	Bündelung der Alarmer eines Kunden, Zuständigkeit, Status, Kommentare und Eskalation
Abschluss	Begründetes Schließen oder Dokumentation eines Verdachtsmeldungsentwurfs
Regelprüfung	Rückwirkende Tests mit historischen Transaktionen; KI-Regelvorschläge als zunächst deaktivierte Entwürfe

Eingaben und Datenqualität

Benötigt werden stabile externe Transaktions- und Kundenkennungen, Konto und Währung, Betrag, Buchungszeitpunkt, Kanal, Gegenpartei und Land. Bei Kartenumsätzen kommen die letzten vier Kartenziffern und die Erfassungsart hinzu. Der Kundenkontext umfasst unter anderem die KYC-Risikoeinstufung.

Zeitstempel, Länderangaben und die Eindeutigkeit der Kennungen sind fachlich entscheidend. Wechselnde Kennungen erzeugen Dubletten; falsche Zeitzeonen verfälschen Zeitfensterregeln. Die Anlieferung muss zum betrachteten Zeitfenster passen. Welche Vorsysteme angebunden werden und welche Verzögerung akzeptabel ist, wird anhand des konkreten Einsatzes festgelegt.

Beispiel: schnelle Weiterleitung von Zahlungseingängen

1. Die Schnittstelle übernimmt die Buchungen und aktualisiert den Auswertungskontext.
2. Eine konfigurierte Regel erkennt das Muster und erzeugt einen Alarm mit den betreffenden Transaktionen.
3. Die KI-Triage ergänzt eine begründete Einschätzung mit Empfehlung; Alarmer werden zum Kundenfall gebündelt.
4. Der Analyst prüft Kundenprofil, Gegenparteien, Zeitstruktur und dokumentierte Erklärungen.
5. Er schließt begründet, eskaliert zur weiteren Prüfung oder dokumentiert einen Meldeentwurf. Seine Begründung bleibt im Prüfpfad erhalten.

Dieser schematische Ablauf verwendet keine echten Kundendaten. Ein Alarm oder ein hoher KI-Risikowert beweist weder Betrug noch Geldwäsche. Die Entscheidung bleibt bei den zuständigen Fachpersonen. Einreichungen erfolgen im dafür vorgesehenen Meldesystem außerhalb dieses Moduls.

Rollen und KI-Kontrolle

Vier Berechtigungsbereiche trennen Lesen, Fallbearbeitung, Regelpflege und Administration. Für die Einführung werden sie den tatsächlichen Rollen des Instituts zugeordnet. Ein lesender Zugriff erlaubt die Prüfung von Fallakten und Prüfpfad, aber keine Falländerung.

Die Triage nutzt den zentralen KI-Dienst der T-NEX-Plattform. Modell und Prompt-Version werden an der Einschätzung festgehalten. Fällt der KI-Dienst aus, bleibt der Alarm mit einem regelbasierten Ersatztext bearbeitbar; der Zusatz .fallback an der Prompt-Version kennzeichnet diesen Zustand. Nach Behebung der Störung kann die Analyse erneut angestoßen werden.

Die Kontrolle durch Analysten umfasst ausdrücklich auch unplausible KI-Begründungen und Unterschiede zwischen Empfehlung und eigener Entscheidung. Modellwahl, Datenfluss, Anbieterbedingungen und Berechtigungen gehören in die konkrete Betriebskonfiguration.

Kalibrierung vor und nach der Einführung

Ein Backtest führt eine Regel gegen historische Transaktionen aus, ohne dadurch automatisch neue Alarmer anzulegen. Geprüfte Transaktionen, Treffer, Trefferquote und zeitliche Verteilung helfen, fachliche Relevanz und Bearbeitungsaufwand einzuschätzen. Treffer werden zusätzlich inhaltlich geprüft. Eine Trefferquote allein ist keine Präzisions- oder Wirksamkeitsmessung.

KI-Regelvorschläge werden als deaktivierte Entwürfe übernommen, fachlich geprüft und rückwirkend getestet. Erst danach wird über ihre Aktivierung entschieden. Gründe für Regeländerungen und Versionen sollten nachvollziehbar bleiben. Schwellenwerte und Bearbeitungsfristen müssen zum Institut passen; dieser Steckbrief definiert dafür keine allgemeingültigen Vorgaben.

Integration, Betrieb und Beschaffung

Das Modul wird in der T-NEX-Plattform aktiviert und benötigt die Datenanbindung, passende Berechtigungen und einen konfigurierten KI-Dienst für KI-Triage. Der dokumentierte Simulator ist für getrennte Schulungs-, Demo- und Abnahmeumgebungen gedacht: Er schreibt synthetische Datensätze in die Modultabellen und gehört nicht in den produktiven Datenbestand.

Im Angebot festzulegen	Konkrete Klärung
Fachlicher Umfang	AML, Karten-/Zahlungsbetrug, Typologien, Zuständigkeiten und Eskalationsweg

Im Angebot festzulegen	Konkrete Klärung
Datenanbindung	Quellen, Feldzuordnung, Kundenstamm, Dublettenerkennung und Lieferverzögerung
KI	Anbieter, Modell, Datenfluss, Freigaben und Verfahren bei Ausfall
Einführung	Getrennte Testumgebung, historische Testdaten, Regelkalibrierung und Analystenschulung
Betrieb	Zielumgebung, Zugriff, Monitoring, Sicherung, Wiederherstellung und Releasepflege
Vertragsumfang	Lizenz, Einführung, Supportzeiten, Reaktionsvereinbarungen und benötigte Nachweise

Die konkrete Hosting-, Datenschutz- und Servicevereinbarung wird durch die fachliche Dokumentation nicht festgelegt. Ebenso wenig ersetzt das Modul die organisatorischen Entscheidungen des Instituts oder dessen Meldeverfahren.

Nachweisgrundlage

Dieser Steckbrief fasst das fachliche Handbuch vom 30. August 2026 zusammen. Der Versionsstand bezeichnet die dokumentierte Anwendung. Das Handbuch ist kein unabhängiger Wirksamkeitstest und enthält keine zugesicherte Erkennungsquote, Verfügbarkeit oder zertifizierte regulatorische Eignung. Ein produktiver Kundeneinsatz wird aus der Modulbeschreibung nicht abgeleitet.

[Produkt und Arbeitsablauf](#) · [Nachweise für Institute](#)

Kontakt: info@t-nex.de